

# NECESSARY CONDITIONS FOR REVERSED DICKSON POLYNOMIALS OF THE SECOND KIND TO BE PERMUTATIONAL

SHAOFANG HONG AND XIAOER QIN  
MATHEMATICAL COLLEGE, SICHUAN UNIVERSITY, CHENGDU 610064, P.R. CHINA

ABSTRACT. In this paper, we present several necessary conditions for the reversed Dickson polynomial  $E_n(1, x)$  of the second kind to be a permutation of  $\mathbb{F}_q$ . In particular, we give explicit evaluation of the sum  $\sum_{a \in \mathbb{F}_q} E_n(1, a)$ .

## 1. Introduction

Let  $p$  be a prime and  $\mathbb{F}_q$  be a finite field of  $q = p^e$  elements, where  $e$  is a positive integer. Associated to any integer  $n \geq 0$  and a parameter  $a \in \mathbb{F}_q$ , the  $n$ -th *Dickson polynomials of the first kind and of the second kind*, denoted by  $D_n(x, a)$  and  $E_n(x, a)$ , are defined by

$$D_n(x, a) := \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}$$

and

$$E_n(x, a) := \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-i}{i} (-a)^i x^{n-2i},$$

respectively. Recently, Wang and Yucas [5] further defined the  $n$ -th *Dickson polynomial of the  $(k+1)$ -th kind*  $D_{n,k}(x, a) \in \mathbb{F}_q[x]$  by

$$D_{n,k}(x, a) := \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-ki}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}.$$

On the other hand, Hou, Mullen, Sellers and Yucas [3] introduced the definition of the *reversed Dickson polynomial of the first kind*, denoted by  $D_n(a, x)$ , as follows

$$D_n(a, x) := \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-x)^i a^{n-2i}.$$

By extending the definition of reversed Dickson polynomials, Wang and Yucas [5] got the definition of the  $n$ -th *reversed Dickson polynomial of the  $(k+1)$ -th kind*  $D_{n,k}(a, x) \in \mathbb{F}_q[x]$ , which is defined by

---

*Date:* April 9, 2014.

*2000 Mathematics Subject Classification.* 11T06, 11C08.

*Key words and phrases.* Permutation polynomial, Reversed Dickson polynomial of the second kind, Finite field, Generating function.

The research was supported partially by National Science Foundation of China Grant #11371260. Emails: sfhong@scu.edu.cn, s-f.hong@tom.com, hongsf02@yahoo.com (S. Hong). qincn328@sina.com (X. Qin).

$$D_{n,k}(a, x) := \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n - ki}{n - i} \binom{n - i}{i} (-x)^i a^{n-2i}.$$

The permutation behavior of Dickson polynomials  $D_n(x, a)$  over finite fields are well known:  $D_n(x, 0) = x^n$  is a permutation polynomial of  $\mathbb{F}_q$  if and only if  $(n, q - 1) = 1$ , and if  $a \neq 0$ , then  $D_n(x, a)$  induces a permutation of  $\mathbb{F}_q$  if and only if  $(n, q^2 - 1) = 1$  (see [4], Theorem 7.16). Meanwhile, there are many results on permutation properties of Dickson polynomial  $E_n(x, a)$  of the second kind, the readers can be referred to [1]. In [5], Wang and Yucas studied the permutational behavior of Dickson polynomials of the third kind  $D_{n,2}(x, 1)$ . They obtained some necessary conditions for  $D_{n,2}(x, 1)$  to be a permutation polynomial of  $\mathbb{F}_q$ .

Hou, Mullen, Sellers and Yucas [3] studied the permutation properties of reversed Dickson polynomial  $D_n(a, x)$  of the first kind. In fact, they showed that  $D_n(a, x)$  is closely related to almost perfect nonlinear (APN) functions, and got several families of permutation polynomials from reversed Dickson polynomials of the first kind. In [2], Hou and Ly found several necessary conditions for reversed Dickson polynomials  $D_n(1, x)$  of the first kind to be a permutation polynomial.

In this paper, we mainly investigate reversed Dickson polynomial of the second kind. We denote by  $E_n(a, x) \in \mathbb{F}_q[x]$  the reversed Dickson polynomial of the second kind, which is defined by

$$E_n(a, x) := \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n - i}{i} (-x)^i a^{n-2i}. \quad (1.1)$$

For  $a \neq 0$ , we write  $x = y(a - y)$  with an indeterminate  $y \neq \frac{a}{2}$ . Then  $E_n(a, x)$  can be rewritten as

$$E_n(a, x) = \frac{y^{n+1} - (a - y)^{n+1}}{2y - a}. \quad (1.2)$$

We will emphasize on the permutation behavior of reversed Dickson polynomials  $E_n(a, x)$  of the second kind over  $\mathbb{F}_q$ . This paper is organized as follows. First in Section 2, we study the properties of the reversed Dickson polynomial  $E_n(a, x)$  of the second kind. Consequently, in Section 3, by introducing the polynomial  $f_m(x) = \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m}{2j+1} x^j$ , we prove several necessary conditions for the reversed Dickson polynomial  $E_n(1, x)$  of the second kind to be a permutation polynomial of  $\mathbb{F}_q$ . It is well known that a function  $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$  is a permutation polynomial of  $\mathbb{F}_q$  if and only if

$$\sum_{a \in \mathbb{F}_q} f(a)^i = \begin{cases} 0, & \text{if } 0 \leq i \leq q - 2, \\ -1, & \text{if } i = q - 1. \end{cases}$$

Thus we would like to know if the sum  $\sum_{a \in \mathbb{F}_q} E_n(1, a)^i$  is computable. We are able to treat with this sum when  $q$  is odd and  $i = 1$ . The final section is devoted to the computation of the sum  $\sum_{a \in \mathbb{F}_q} E_n(1, a)$ .

## 2. Reversed Dickson polynomials of the second kind

In this section, we mainly study properties of reversed Dickson polynomials of the second kind. If  $a = 0$ , then

$$E_n(0, x) = \begin{cases} 0, & \text{if } n \text{ is odd,} \\ (-x)^k, & \text{if } n = 2k, k \text{ is nonnegative integer.} \end{cases}$$

Hence  $E_n(0, x)$  is a PP (permutation polynomial) of  $\mathbb{F}_q$  if and only  $n = 2k$  with  $(k, q-1) = 1$ . In what follows we assume that  $a \in \mathbb{F}_q^*$ . By a trivial fact that  $f(x)$  is a PP of  $\mathbb{F}_q$  if and only if  $cf(dx)$  is a PP of  $\mathbb{F}_q$  for any given  $c, d \in \mathbb{F}_q^*$ , we can easily deduce the following result.

**Theorem 2.1.** *Let  $a, b \in \mathbb{F}_q^*$ . Then  $E_n(a, x) = \frac{a^n}{b^n} E_n(b, \frac{b^2}{a^2}x)$ . Furthermore,  $E_n(a, x)$  is a PP of  $\mathbb{F}_q$  if and only if  $E_n(1, x)$  is a PP of  $\mathbb{F}_q$ .*

*Proof.* First by the definition (1.1), we have

$$\begin{aligned} \frac{a^n}{b^n} E_n\left(b, \frac{b^2}{a^2}x\right) &= \frac{a^n}{b^n} \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-i}{i} \left(-\frac{b^2}{a^2}x\right)^i b^{n-2i} \\ &= \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-i}{i} (-x)^i b^{n-2i} \left(\frac{b}{a}\right)^{2i-n} \\ &= E_n(a, x). \end{aligned}$$

So the first part is proved.

To show the second part, one notices that  $E_n(a, x) = a^n E_n(1, \frac{x}{a^2})$ . Since  $a \in \mathbb{F}_q^*$ , one has  $a^n, \frac{1}{a^2} \in \mathbb{F}_q^*$ . It follows that  $E_n(a, x)$  is a PP of  $\mathbb{F}_q$  if and only  $E_n(1, x)$  is a PP of  $\mathbb{F}_q$ . This concludes the proof of second part. Hence Theorem 2.1 is proved.  $\square$

By Theorem 2.1, it is easy to see that to study the permutation behavior of reversed Dickson polynomial  $E_n(a, x)$  of the second kind, one needs only to consider that of  $E_n(1, x)$ . In the following, we list some basic facts about the reversed Dickson polynomial  $E_n(1, x)$  of the second kind.

**Theorem 2.2.** *Let  $p$  be an odd prime,  $n$  and  $r$  be positive integers. Each of the following is true:*

- (1). *We have  $E_n(1, x(1-x)) = \frac{x^{n+1} - (1-x)^{n+1}}{2x-1}$  if  $x \neq \frac{1}{2}$  and  $E_n(1, \frac{1}{4}) = \frac{n+1}{2^n}$ .*
- (2). *If  $\gcd(p, n) = 1$ , then  $E_{np^r-1}(1, x) = (E_{n-1}(1, x))^{p^r} (1-4x)^{\frac{p^r-1}{2}}$ .*
- (3). *If  $n_1$  and  $n_2$  are positive integers such that  $n_1 \equiv n_2 \pmod{q^2-1}$ , then  $E_{n_1}(1, x_0) = E_{n_2}(1, x_0)$  for any  $x_0 \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$ .*

*Proof.* (1). Clearly, the first identity follows from (1.2). To prove the second one, we notice that by (2.3) of [1] (see page 226 of [1]), we have  $E_n(2, 1) = n+1$ . But Theorem 2.1 tells us that  $E_n(2, 1) = 2^n E_n(1, \frac{1}{4})$ . Thus  $E_n(1, \frac{1}{4}) = \frac{n+1}{2^n}$  as required.

(2). Writing  $x = y(1-y)$  with  $y \neq \frac{1}{2}$  being an indeterminate gives us that  $1-4x = (2y-1)^2$ . So by part (1), one derives that

$$\begin{aligned} E_{np^r-1}(1, x) &= E_{np^r-1}(1, y(1-y)) \\ &= \frac{y^{np^r} - (1-y)^{np^r}}{2y-1} \\ &= \left( \frac{y^n - (1-y)^n}{2y-1} \right)^{p^r} (2y-1)^{p^r-1} \\ &= (E_{n-1}(1, y(1-y)))^{p^r} (2y-1)^{p^r-1} \\ &= E_{n-1}(1, x)^{p^r} (1-4x)^{\frac{p^r-1}{2}}. \end{aligned}$$

Particularly, if  $x = \frac{1}{4}$ , then by part (1), we have

$$E_{np^r-1}(1, x) = E_{np^r-1}\left(1, \frac{1}{4}\right) = \frac{np^r}{2^{np^r-1}} = 0 = (E_{n-1}(1, x))^{p^r} (1-4x)^{\frac{p^r-1}{2}}$$

as desired. Part (2) is proved.

(3). For each  $x_0 \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$ , one may write  $y_0 \in \mathbb{F}_{q^2} \setminus \{\frac{1}{2}\}$  such that  $x_0 = y_0(1 - y_0)$ . Thus

$$\begin{aligned} E_{n_1}(1, x_0) &= E_{n_1}(1, y_0(1 - y_0)) \\ &= \frac{y_0^{n_1+1} - (1 - y_0)^{n_1+1}}{2y_0 - 1} \\ &= \frac{y_0^{n_2+1} - (1 - y_0)^{n_2+1}}{2y_0 - 1} \\ &= E_{n_2}(1, x_0). \end{aligned}$$

This ends the proof of Theorem 2.2.  $\square$

**Remark.** When  $p = 2$ , we have

$$E_n(1, x(1 - x)) = x^{n+1} + (1 - x)^{n+1} = D_{n+1}(1, x(1 - x)).$$

In [3], Hou et al. discussed some connections between reversed Dickson PPs of  $\mathbb{F}_q$  and APN functions of  $\mathbb{F}_q$ , and obtained several families of reversed Dickson PPs. Throughout the reminder of this article, unless specified,  $p$  is always assumed to be an odd prime.

By [5], we know that  $E_n(x, a) = xE_{n-1}(x, a) - aE_{n-2}(x, a)$  holds for any integer  $n \geq 2$ . Regarding  $E_n(1, x)$ , we have the following result.

**Proposition 2.1.** *Let  $p$  be an odd prime and  $n \geq 2$  be an integer. Then  $E_n(1, x) = E_{n-1}(1, x) - xE_{n-2}(1, x)$ .*

*Proof.* First we consider the case  $x \neq \frac{1}{4}$ . For this case, one may let  $x = y(1 - y)$  with  $y$  being an indeterminate and  $y \neq \frac{1}{2}$ . Then by Theorem 2.2 (1), we have

$$\begin{aligned} &E_{n-1}(1, y(1 - y)) - y(1 - y)E_{n-2}(1, y(1 - y)) \\ &= \frac{y^n - (1 - y)^n}{2y - 1} - y(1 - y) \frac{y^{n-1} - (1 - y)^{n-1}}{2y - 1} \\ &= \frac{y^n - (1 - y)^n}{2y - 1} - \frac{y^n(1 - y) - y(1 - y)^n}{2y - 1} \\ &= \frac{y^{n+1} - (1 - y)^{n+1}}{2y - 1} = E_n(1, y(1 - y)). \end{aligned}$$

For the case  $x = \frac{1}{4}$ , by Theorem 2.2 (1), we infer that

$$E_{n-1}\left(1, \frac{1}{4}\right) - \frac{1}{4}E_{n-2}\left(1, \frac{1}{4}\right) = \frac{n}{2^{n-1}} - \frac{n-1}{2^n} = \frac{n+1}{2^n} = E_n\left(1, \frac{1}{4}\right).$$

Thus Proposition 2.2 is proved.  $\square$

Using this recursion, we can obtain the generating function of the reversed Dickson polynomial  $E_n(1, x)$  of the second kind as follows.

**Proposition 2.2.** *The generating function of  $E_n(1, x)$  is given by:*

$$\sum_{n=0}^{\infty} E_n(1, x)t^n = \frac{1}{1 - t + xt^2}.$$

*Proof.* By Proposition 2.1, we have

$$\begin{aligned}
& (1 - t + xt^2) \sum_{n=0}^{\infty} E_n(1, x) t^n \\
&= \sum_{n=0}^{\infty} E_n(1, x) t^n - \sum_{n=0}^{\infty} E_n(1, x) t^{n+1} + x \sum_{n=0}^{\infty} E_n(1, x) t^{n+2} \\
&= 1 + t - t + \sum_{n=0}^{\infty} (E_{n+2}(1, x) - E_{n+1}(1, x) + x E_n(1, x)) t^{n+2} = 1.
\end{aligned}$$

Thus the desired result follows immediately.  $\square$

In the following, by using the reversed Dickson polynomial  $E_n(1, x)$  of the second kind, we obtain some PPs of  $\mathbb{F}_q$ .

**Proposition 2.3.** *Let  $p$  be an odd prime and  $k$  be a positive integer. Then we have*

$$E_{p^k-1}(1, x) = (1 - 4x)^{\frac{p^k-1}{2}}.$$

*Proof.* First putting  $x = y(1 - y)$  with an indeterminate  $y \neq \frac{1}{2}$ . By Theorem 2.2 (1), one has

$$\begin{aligned}
E_{p^k-1}(1, x) &= E_{p^k-1}(1, y(1 - y)) = \frac{y^{p^k} - (1 - y)^{p^k}}{2y - 1} = \frac{(2y - 1)^{p^k}}{2y - 1} \\
&= (2y - 1)^{p^k-1} = [(2y - 1)^2]^{\frac{p^k-1}{2}} = [-4y(1 - y) + 1]^{\frac{p^k-1}{2}} = (-4x + 1)^{\frac{p^k-1}{2}}.
\end{aligned}$$

Also Theorem 2.2 (1) implies that

$$E_{p^k-1}\left(1, \frac{1}{4}\right) = \frac{p^k}{2^{p^k-1}} = 0 = \left(1 - 4 \times \frac{1}{4}\right)^{\frac{p^k-1}{2}}$$

as one desires.  $\square$

**Lemma 2.1.** [4] *Each of the following is true:*

- (1). *Every linear polynomial over  $\mathbb{F}_q$  is a PP of  $\mathbb{F}_q$ .*
- (2). *The monomial  $x^n$  is a PP of  $\mathbb{F}_q$  if and only if  $(n, q - 1) = 1$ .*

By Proposition 2.3 and Lemma 2.1, the following result follows immediately.

**Corollary 2.1.** *Let  $p$  be an odd prime and  $q = p^e$ . Let  $e$  and  $k$  be positive integers with  $1 \leq k \leq e$ . Then  $E_{p^k-1}(1, x)$  is a PP of  $\mathbb{F}_q$  if and only if  $(\frac{p^k-1}{2}, q - 1) = 1$ .*

**Lemma 2.2.** [3] *Let  $x \in \mathbb{F}_{q^2}$ . Then  $x(1 - x) \in \mathbb{F}_q$  if and only if  $x^q = x$  or  $x^q = 1 - x$ .*

We define

$$V := \{x \in \mathbb{F}_{q^2} : x^q = 1 - x\}.$$

Then  $\mathbb{F}_q \cap V = \{\frac{1}{2}\}$ . We can now give a characterization for  $E_n(1, x)$  to be a PP.

**Theorem 2.3.** *Let  $p$  be an odd prime and  $f : y \mapsto \frac{y^{n+1} - (1-y)^{n+1}}{2y-1}$  be a mapping on  $(\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$ . Then  $E_n(1, x)$  is a PP of  $\mathbb{F}_q$  if and only if  $f$  is 2-to-1 and  $f(y) \neq \frac{n+1}{2^n}$  for any  $y \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$ .*

*Proof.* First to show the sufficiency part, we choose two elements  $x_1$  and  $x_2 \in \mathbb{F}_q$  satisfying that  $E_n(1, x_1) = E_n(1, x_2)$ . Since  $x_1, x_2 \in \mathbb{F}_q$ , there exist  $y_1, y_2 \in \mathbb{F}_{q^2}$  such that  $x_1 = y_1(1 - y_1)$  and  $x_2 = y_2(1 - y_2)$ . Then by Lemma 2.2, we know that  $y_1, y_2 \in \mathbb{F}_q \cup V$ . Consider the following cases.

CASE 1. Exactly one of  $x_1$  and  $x_2$  is equal to  $\frac{1}{4}$ . Without loss of any generality, one may let  $x_1 = \frac{1}{4}$ . Then  $y_1 = \frac{1}{2}$ . Since  $E_n(1, x_1) = E_n(1, x_2)$ , it follows from Theorem 2.2 (1) that  $E_n(1, x_2) = E_n(1, \frac{1}{4}) = \frac{n+1}{2^n}$ . Claim that  $x_2 = \frac{1}{4}$ . Otherwise, we have  $x_2 \neq \frac{1}{4}$ .

It follows that  $y_2 \neq \frac{1}{2}$ . Since  $f(y) \neq \frac{n+1}{2^n}$  for any  $y \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$ , by Theorem 2.2 (1) we derive that

$$E_n(1, x_2) = E_n(1, y_2(1 - y_2)) = \frac{y_2^{n+1} - (1 - y_2)^{n+1}}{2y_2 - 1} = f(y_2) \neq \frac{n+1}{2^n},$$

which arrives at a contradiction. Hence we must have  $x_2 = \frac{1}{4}$ . The claim is proved. Now by the claim, one has  $x_1 = x_2$ .

CASE 2.  $x_1 \neq \frac{1}{4}$  and  $x_2 \neq \frac{1}{4}$ . Since  $E_n(1, x_1) = E_n(1, x_2)$ , we have  $f(y_1) = f(y_2)$ . Since  $f$  is a 2-to-1 mapping on  $(\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$ , it follows that  $y_1 = y_2$  or  $y_1 = 1 - y_2$ . This implies that  $x_1 = x_2$ . Hence  $E_n(1, x)$  is a PP of  $\mathbb{F}_q$ . Therefore the sufficiency part is proved.

Let us now prove the necessity part. Assume that  $E_n(1, x)$  is a PP of  $\mathbb{F}_q$ . We choose two elements  $y_1, y_2 \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$  such that  $f(y_1) = f(y_2)$ , namely,

$$\frac{y_1^{n+1} - (1 - y_1)^{n+1}}{2y_1 - 1} = \frac{y_2^{n+1} - (1 - y_2)^{n+1}}{2y_2 - 1}. \quad (2.1)$$

Since  $y_1, y_2 \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$ , by Lemma 2.2 one has  $y_1(1 - y_1) \in \mathbb{F}_q$  and  $y_2(1 - y_2) \in \mathbb{F}_q$ . Then by Theorem 2.2 (1), (2.1) infers that

$$E_n(1, y_1(1 - y_1)) = E_n(1, y_2(1 - y_2)).$$

But  $E_n(1, x)$  is a PP of  $\mathbb{F}_q$ , we then have  $y_1(1 - y_1) = y_2(1 - y_2)$ . Thus one can immediately get that  $y_1 = y_2$  or  $y_1 = 1 - y_2$ . Thus  $f$  is a 2-to-1 mapping on  $(\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$ .

Finally, picking  $y \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$ , it follows from Lemma 2.2 that  $y(1 - y) \in \mathbb{F}_q$  and  $y(1 - y) \neq \frac{1}{2}(1 - \frac{1}{2})$ . Since  $E_n(1, x)$  is a PP of  $\mathbb{F}_q$ , it follows that

$$E_n(1, y(1 - y)) \neq E_n\left(1, \frac{1}{2}\left(1 - \frac{1}{2}\right)\right).$$

Note that  $E_n(1, \frac{1}{2}(1 - \frac{1}{2})) = \frac{n+1}{2^n}$ . Then by Theorem 2.2 (1) one has

$$\frac{y^{n+1} - (1 - y)^{n+1}}{2y - 1} \neq \frac{n+1}{2^n}.$$

Thus  $f(y) \neq \frac{n+1}{2^n}$  for any  $y \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$ . The necessity part is proved.

This completes the proof of Theorem 2.3.  $\square$

### 3. Necessary conditions for $E_n(1, x)$ to be permutational

In the present section, we study some necessary conditions on  $n$  for  $E_n(1, x)$  to be a PP of  $\mathbb{F}_q$ . Note that  $E_n(1, 0) = 1$ . By the following recursive relation

$$\begin{cases} E_0(1, 1) = 1, \\ E_1(1, 1) = 1, \\ E_{n+2}(1, 1) = E_{n+1}(1, 1) - E_n(1, 1), \end{cases}$$

it follows that

$$E_2(1, 1) = 0, E_3(1, 1) = -1, E_4(1, 1) = -1, E_5(1, 1) = 0.$$

The sequence  $\{E_n(1, 1) \mid n \in \mathbb{N}\}$  has period 6 and

$$E_n(1, 1) = \begin{cases} 0, & \text{if } n \equiv 2, 5 \pmod{6}; \\ 1, & \text{if } n \equiv 0, 1 \pmod{6}; \\ -1, & \text{if } n \equiv 3, 4 \pmod{6}. \end{cases}$$

**Theorem 3.1.** *Assume that  $E_n(1, x)$  is a PP of  $\mathbb{F}_q$ . If  $p = 2$ , then  $3 \mid (n+1)$ ; If  $p$  is an odd prime, then  $n \not\equiv 0, 1 \pmod{6}$ .*

*Proof.* By comparing  $E_n(1, 0)$  with  $E_n(1, 1)$ , we get the desired result immediately.  $\square$

Let  $m \geq 0$  be an integer. We define the polynomial  $f_m(x)$  by

$$f_m(x) := \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m}{2j+1} x^j \in \mathbb{Z}[x].$$

We have the following relation between  $f_{n+1}(x)$  and  $E_n(1, x)$ .

**Theorem 3.2.** *Let  $p$  be an odd prime. Then  $E_n(1, x) = \frac{1}{2^n} f_{n+1}(1 - 4x)$ . Consequently,  $E_n(1, x)$  is a PP of  $\mathbb{F}_q$  if and only if  $f_{n+1}(x)$  is a PP of  $\mathbb{F}_q$ .*

*Proof.* First we write  $x = y(1 - y)$  with an indeterminate  $y \neq \frac{1}{2}$ . Let  $u = 2y - 1$ . Then by Theorem 2.2 (1), we derive that

$$\begin{aligned} E_n(1, x) &= E_n(1, y(1 - y)) \\ &= \frac{1}{u} [y^{n+1} - (1 - y)^{n+1}] \\ &= \frac{1}{u} \left[ \left( \frac{1+u}{2} \right)^{n+1} - \left( \frac{1-u}{2} \right)^{n+1} \right] \\ &= \frac{1}{2^{n+1}u} [(1+u)^{n+1} - (1-u)^{n+1}] \\ &= \frac{1}{2^n u} \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n+1}{2j+1} u^{2j+1} \\ &= \frac{1}{2^n} \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n+1}{2j+1} u^{2j} \\ &= \frac{1}{2^n} f_{n+1}(u^2) \\ &= \frac{1}{2^n} f_{n+1}(1 - 4y(1 - y)) \\ &= \frac{1}{2^n} f_{n+1}(1 - 4x). \end{aligned}$$

Next let  $x = \frac{1}{4}$ . Then we obtain that

$$E_n(1, x) = E_n\left(1, \frac{1}{4}\right) = \frac{n+1}{2^n} = \frac{1}{2^n} f_{n+1}(0) = \frac{1}{2^n} f_{n+1}(1 - 4x).$$

So the first part is proved.

Since  $\frac{1}{2^n} \in \mathbb{F}_q^*$  and  $1 - 4x$  is linear, we know that  $E_n(1, x)$  is a PP of  $\mathbb{F}_q$  if and only if  $f_{n+1}(x)$  is a PP of  $\mathbb{F}_q$ . The proof of Theorem 3.2 is complete.  $\square$

Using the relation between  $f_{n+1}(x)$  and  $E_n(1, x)$  is described in Theorem 3.2, we can get the following results.

**Theorem 3.3.** *Let  $p$  be an odd prime and  $m$  be a nonnegative integer with  $p \nmid (m+1)$ . If  $E_{2m+1}(1, x)$  is a PP of  $\mathbb{F}_q$ , then  $m$  is odd and  $(m, q-1) = 1$ .*

*Proof.* We suppose that  $E_{2m+1}(1, x)$  is a PP of  $\mathbb{F}_q$ . Then it follows from Theorem 3.2 that  $f_{2m+2}(x)$  is a PP of  $\mathbb{F}_q$ . So we can choose an element  $x_0 \in \mathbb{F}_q$  such that  $f_{2m+2}(x_0) = 0$ . Since  $f_{2m+2}(0) = 2m + 2 \neq 0$  and  $f_{2m+2}(x)$  is a PP of  $\mathbb{F}_q$ , we deduce that  $x_0 \neq 0$ .

On the other hand, one can easily check that  $f_{2m+2}(x) = x^m f_{2m+2}(x^{-1})$ . Namely,  $f_{2m+2}(x)$  is a self-reciprocal polynomial. Then by  $f_{2m+2}(x_0) = 0$  and  $x_0 \neq 0$ , we have that  $f_{2m+2}(x_0) = f_{2m+2}(x_0^{-1}) = 0$ . Since  $f_{2m+2}(x)$  is a PP of  $\mathbb{F}_q$ , we derive that  $x_0 = x_0^{-1}$ , i.e.,  $x_0 = \pm 1$ . But

$$f_{2m+2}(1) = \sum_{j=0}^m \binom{2m+2}{2j+1} = 2^{2m+1} \neq 0.$$

Then  $x_0$  must equal  $-1$ . Thus we have

$$\begin{aligned} 0 = f_{2m+2}(-1) &= \sum_{j \equiv 1 \pmod{4}} \binom{2m+2}{j} - \sum_{j \equiv 3 \pmod{4}} \binom{2m+2}{j} \\ &= \frac{1}{2} [i(1-i)^{2m+2} - i(1+i)^{2m+2}] \\ &= \frac{1}{2} i [(\sqrt{2}e^{\frac{-\pi i}{4}})^{2m+2} - (\sqrt{2}e^{\frac{\pi i}{4}})^{2m+2}] \\ &= 2^m i [e^{\frac{-(m+1)\pi i}{2}} - e^{\frac{(m+1)\pi i}{2}}]. \end{aligned}$$

It follows that  $e^{\frac{-(m+1)\pi i}{2}} - e^{\frac{(m+1)\pi i}{2}} = 0$ . Hence  $m+1$  is even. In other words,  $m$  is odd.

Let us show that  $(m, q-1) = 1$ . Assume that  $(m, q-1) = d \geq 3$ . Let  $\theta \in \mathbb{F}_q^*$  satisfy  $o(\theta) = d$ , where  $o(\theta)$  means the order of  $\theta$  in  $\mathbb{F}_q^*$ . Since  $f_{2m+2}(x)$  is self-reciprocal, one has  $f_{2m+2}(\theta) = \theta^m f_{2m+2}(\theta^{-1}) = f_{2m+2}(\theta^{-1})$ . But  $\theta \neq \theta^{-1}$ , which contradicts with the fact that  $f_{2m+2}(x)$  is a PP of  $\mathbb{F}_q$ . Thus  $(m, q-1) = 1$  as required.

This completes the proof of Theorem 3.3.  $\square$

The following lemmas are needed in the reminder of this section.

**Lemma 3.1.** *Let  $p$  be an odd prime and  $q$  be the power of  $p$ . Let  $n \geq 1$  be an integer with  $n \equiv 1 \pmod{4}$ . Then  $(n+1, q-1)(n+1, q+1) = 2(n+1, q^2-1)$ .*

*Proof.* Since  $q$  is odd and  $n \equiv 1 \pmod{4}$ , we have  $(n+1, q-1, q+1) = 2$ . Let  $(n+1, q-1) = 2d_1$  and  $(n+1, q+1) = 2d_2$ . Then  $d_1$  and  $d_2$  are two odd integer,  $(d_1, d_2) = 1$  and  $n+1 = 2d_1d_2l$  for some positive integer  $l$ . Since  $n \equiv 1 \pmod{4}$ , it follows that  $n+1 \equiv 2 \pmod{4}$  and  $(l, 2) = 1$ . Let  $q-1 = 2d_1u_1$  and  $q+1 = 2d_2u_2$ . Then one can deduce that  $(d_2l, u_1) = 1$  and  $(d_1l, u_2) = 1$ . It implies that  $(l, u_1) = (l, u_2) = 1$ . Thus  $(l, 2u_1u_2) = 1$ . It then follows that

$$\begin{aligned} (n+1, q-1)(n+1, q+1) &= 4d_1d_2 = 4d_1d_2(l, 2u_1u_2) \\ &= 2(2d_1d_2l, 4d_1d_2u_1u_2) = 2(n+1, q^2-1) \end{aligned}$$

as desired. Lemma 3.1 is proved.  $\square$

**Lemma 3.2.** [2] *Let  $\theta \notin \{0, 1\}$  be in some extension of  $\mathbb{F}_q$  and let  $y = \frac{\theta+1}{\theta-1}$ . Then  $y^2 \in \mathbb{F}_q$  if and only if  $\theta^{q+1} = 1$  or  $\theta^{q-1} = 1$ .*

**Theorem 3.4.** *Let  $p > 3$  be an odd prime and  $n \geq 0$  be an integer with  $3 \mid (n+1)$  and  $n \equiv 1 \pmod{4}$ . If  $E_n(1, x)$  is a PP of  $\mathbb{F}_q$ , then  $(n+1, q^2-1) = 6$ .*

*Proof.* Since  $p > 3$ , we get that  $q \equiv 1$  or  $2 \pmod{3}$ . Thus  $3 \mid (q+1)$  or  $3 \mid (q-1)$ . Namely, 3 divides  $q^2-1$ . Since  $n+1$  is divisible by 3, we get that  $3 \mid (n+1, q^2-1)$ .



But  $p$  and  $n$  are odd integers, we deduce that  $2 \mid (n+1, q^2-1)$ . Thus  $6 \mid (n+1, q^2-1)$ . That is,  $(n+1, q^2-1) \geq 6$ . In what follows we show that  $(n+1, q^2-1) = 6$ .

Assume that  $(n+1, q^2-1) > 6$ . Writing

$$E := \{\theta \in \mathbb{F}_{q^2}^* : \theta \neq 1, \theta^{(n+1, q+1)} = 1 \text{ or } \theta^{(n+1, q-1)} = 1\}$$

gives us that

$$|E| = (n+1, q+1) + (n+1, q-1) - 3.$$

Then it follows from Lemma 3.1 and the assumption  $(n+1, q^2-1) > 6$  that

$$(n+1, q-1)(n+1, q+1) = 2(n+1, q^2-1) > 12.$$

From this inequality one can derive that  $|E| > 4$ .

We take three distinct elements  $\theta_1, \theta_2, \theta_3 \in E$ . Let  $i$  be an integer with  $1 \leq i \leq 3$ . Then  $\theta_i^{q+1} = 1$  or  $\theta_i^{q-1} = 1$ . Let  $y_i = \frac{\theta_i+1}{\theta_i-1}$ . It follows from Lemma 3.2 that  $y_i^2 \in \mathbb{F}_q$ . Since  $y_i = \frac{\theta_i+1}{\theta_i-1}$ , we have  $\frac{y_i+1}{y_i-1} = \theta_i$ . Thus  $(\frac{y_i+1}{y_i-1})^{n+1} = 1$ . Namely,  $(y_i+1)^{n+1} = (y_i-1)^{n+1}$ . So by

$$f_{n+1}(y_i^2) = \frac{1}{2y_i}[(1+y_i)^{n+1} - (1-y_i)^{n+1}],$$

we deduce that  $f_{n+1}(y_i^2) = 0$ . Since  $\theta_1, \theta_2, \theta_3 \in E$  are distinct, it is easy to check that  $y_1, y_2$  and  $y_3$  are distinct. Thus at least two of  $y_1^2, y_2^2$  and  $y_3^2$  are distinct. But

$$f_{n+1}(y_1^2) = f_{n+1}(y_2^2) = f_{n+1}(y_3^2) = 0.$$

Hence  $f_{n+1}(x)$  is not a PP of  $\mathbb{F}_q$ . By Theorem 3.2, one derives that  $E_n(1, x)$  is not a PP of  $\mathbb{F}_q$ . This is a contradiction. Thus  $(n+1, q^2-1) = 6$  as desired.

The proof of Theorem 3.4 is complete.  $\square$

**Theorem 3.5.** *Let  $p > 3$  be an odd prime and  $n \geq 0$  be an integer with  $3 \nmid (n+1)$  and  $n \equiv 1 \pmod{4}$ . If  $E_n(1, x)$  is a PP of  $\mathbb{F}_q$ , then  $(n+1, q^2-1) = 2$ .*

*Proof.* Since 3 does not divide  $n+1$ , we have  $2 \mid (n+1, q^2-1)$ . Let us show that  $(n+1, q^2-1) = 2$ . Assume that  $(n+1, q^2-1) > 2$ . Then  $(n+1, q^2-1) \geq 6$ . Let

$$E := \{\theta \in \mathbb{F}_{q^2}^* : \theta \neq 1, \theta^{(n+1, q+1)} = 1 \text{ or } \theta^{(n+1, q-1)} = 1\}.$$

Then

$$|E| = (n+1, q+1) + (n+1, q-1) - 3.$$

By Lemma 3.1, one has

$$(n+1, q-1)(n+1, q+1) = 2(n+1, q^2-1) \geq 12.$$

Then one derives that  $|E| \geq 4$ . Then in the similar way as in the proof of Theorem 3.4, we can show that  $f_{n+1}(x)$  is not a PP of  $\mathbb{F}_q$ . Then by Theorem 3.2 we obtain that  $E_n(1, x)$  is not a PP of  $\mathbb{F}_q$ , which is a contradiction. We then conclude that  $(n+1, q^2-1) = 2$ .

This ends the proof of Theorem 3.5.  $\square$

#### 4. Computation of $\sum_{a \in \mathbb{F}_q} E_n(1, a)$

In this section, we compute the sum  $\sum_{a \in \mathbb{F}_q} E_n(1, a)$ . By Proposition 2.2, we have

$$\begin{aligned}
\sum_{n \geq 0} E_n(1, x) t^n &= \frac{1}{1 - t + xt^2} \\
&= \frac{1}{1 - t} \frac{1}{1 - \frac{t^2 x}{t - 1}} \\
&= \frac{1}{1 - t} \sum_{k \geq 0} \left( \frac{t^2}{t - 1} \right)^k x^k \\
&= \frac{1}{1 - t} \left[ 1 + \sum_{k=1}^{q-1} \sum_{l \geq 0} \left( \frac{t^2}{t - 1} \right)^{k+l(q-1)} x^{k+l(q-1)} \right] \\
&\equiv \frac{1}{1 - t} \left[ 1 + \sum_{k=1}^{q-1} \sum_{l \geq 0} \left( \frac{t^2}{t - 1} \right)^{k+l(q-1)} x^k \right] \pmod{x^q - x} \\
&= \frac{1}{1 - t} \left[ 1 + \sum_{k=1}^{q-1} \frac{\left( \frac{t^2}{t - 1} \right)^k}{1 - \left( \frac{t^2}{t - 1} \right)^{q-1}} x^k \right] \\
&= \frac{1}{1 - t} \left[ 1 + \sum_{k=1}^{q-1} \frac{(t - 1)^{q-1-k} t^{2k}}{(t - 1)^{q-1} - t^{2(q-1)}} x^k \right]. \tag{4.1}
\end{aligned}$$

On the other hand, by Theorem 2.2 (3), we know that if  $n_1 \equiv n_2 \pmod{q^2 - 1}$ , then  $E_{n_1}(1, x) = E_{n_2}(1, x)$  for any  $x \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$ . It then follows that

$$\begin{aligned}
\sum_{n \geq 0} E_n(1, x) t^n &= 1 + \sum_{n=1}^{q^2-1} \sum_{l \geq 0} E_{n+l(q^2-1)}(1, x) t^{n+l(q^2-1)} \\
&\equiv 1 + \sum_{n=1}^{q^2-1} E_n(1, x) \sum_{l \geq 0} t^{n+l(q^2-1)} \pmod{x^q - x} \\
&= 1 + \frac{1}{1 - t^{q^2-1}} \sum_{n=1}^{q^2-1} E_n(1, x) t^n. \tag{4.2}
\end{aligned}$$

Now (4.1) together with (4.2) implies that

$$\begin{aligned}
&\sum_{n=1}^{q^2-1} E_n(1, x) t^n \\
&\equiv (1 - t^{q^2-1}) \left( \frac{1}{1 - t} - 1 \right) + \frac{1 - t^{q^2-1}}{1 - t} \sum_{k=1}^{q-1} \frac{(t - 1)^{q-1-k} t^{2k}}{(t - 1)^{q-1} - t^{2(q-1)}} x^k \pmod{x^q - x} \\
&= \frac{t(1 - t^{q^2-1})}{1 - t} + h(t) \sum_{k=1}^{q-1} (t - 1)^{q-1-k} t^{2k} x^k, \tag{4.3}
\end{aligned}$$

where

$$h(t) := \frac{t^{q^2-1} - 1}{(t - 1)^q - (t - 1)t^{2(q-1)}}.$$

We need the following well-known result.

**Lemma 4.1.** [4] *Let  $u_0, u_1, \dots, u_{q-1}$  be the all elements of  $\mathbb{F}_q$ . Then*

$$\sum_{i=0}^{q-1} u_i^k = \begin{cases} 0, & \text{if } 0 \leq k \leq q-2; \\ -1, & \text{if } k = q-1. \end{cases}$$

Then by Lemma 4.1 and (4.3), we obtain that

$$\begin{aligned} & \sum_{n=1}^{q^2-1} \left( \sum_{a \in \mathbb{F}_q} E_n(1, a) \right) t^n \\ &= \sum_{n=1}^{q^2-1} E_n\left(1, \frac{1}{4}\right) t^n + \sum_{n=1}^{q^2-1} \left( \sum_{a \in \mathbb{F}_q \setminus \{\frac{1}{4}\}} E_n(1, a) \right) t^n \\ &= \sum_{n=1}^{q^2-1} E_n\left(1, \frac{1}{4}\right) t^n + \sum_{a \in \mathbb{F}_q \setminus \{\frac{1}{4}\}} \sum_{n=1}^{q^2-1} E_n(1, a) t^n \\ &= \sum_{n=1}^{q^2-1} \frac{n+1}{2^n} t^n + \sum_{a \in \mathbb{F}_q \setminus \{\frac{1}{4}\}} \frac{t(1-t^{q^2-1})}{1-t} + h(t) \sum_{k=1}^{q-1} (t-1)^{q-1-k} t^{2k} \sum_{a \in \mathbb{F}_q \setminus \{\frac{1}{4}\}} a^k \\ &= \sum_{n=1}^{q^2-1} \frac{n+1}{2^n} t^n + (q-1) \frac{t(1-t^{q^2-1})}{1-t} + h(t) \sum_{k=1}^{q-1} (t-1)^{q-1-k} t^{2k} \sum_{a \in \mathbb{F}_q} a^k \\ &\quad - h(t) \sum_{k=1}^{q-1} (t-1)^{q-1-k} t^{2k} \left(\frac{1}{4}\right)^k \\ &= \sum_{n=1}^{q^2-1} \frac{n+1}{2^n} t^n - \frac{t(1-t^{q^2-1})}{1-t} - h(t) t^{2(q-1)} - h(t) \sum_{k=1}^{q-1} (t-1)^{q-1-k} t^{2k} \left(\frac{1}{4}\right)^k. \end{aligned} \quad (4.4)$$

However, we have

$$h(t) = \frac{t^{q^2-1} - 1}{(1-t^{q-1})(t^q - t^{q-1} - 1)} = \frac{t^{q^2} - t}{(t-t^q)(t^q - t^{q-1} - 1)} := \frac{\sum_{i=0}^{q^2-q} b_i t^i}{t^q - t^{q-1} - 1}. \quad (4.5)$$

Evidently,  $\sum_{i=0}^{q^2-q} b_i t^i = -1 - (t-t^q)^{q-1}$ . Then the binomial expansion theorem applied to  $(t-t^q)^{q-1}$  gives us the following result.

**Proposition 4.1.** *For  $0 \leq i \leq q^2 - q$ , write  $i = \alpha + \beta q$  with  $0 \leq \alpha, \beta \leq q-1$ . Then*

$$b_i = \begin{cases} (-1)^{\beta+1} \binom{q-1}{\beta}, & \text{if } \alpha + \beta = q-1; \\ -1, & \text{if } \alpha = \beta = 0; \\ 0, & \text{otherwise.} \end{cases}$$

Let  $a_n := \sum_{a \in \mathbb{F}_q} E_n(1, a)$  for  $1 \leq n \leq q^2 - 1$ . Then by (4.4) and (4.5), we arrive at

$$\sum_{n=1}^{q^2-1} \left( a_n - \frac{n+1}{2^n} \right) t^n = -\frac{t(1-t^{q^2-1})}{1-t} - \frac{\sum_{i=0}^{q^2-q} b_i t^i}{t^q - t^{q-1} - 1} \left( t^{2(q-1)} + \sum_{k=1}^{q-1} (t-1)^{q-1-k} t^{2k} \left(\frac{1}{4}\right)^k \right).$$

It infers that

$$\begin{aligned}
& (t^q - t^{q-1} - 1) \sum_{n=1}^{q^2-1} \left( a_n - \frac{n+1}{2^n} \right) t^n \\
= & (1 - t^q + t^{q-1}) \sum_{i=1}^{q^2-1} t^i - \left( t^{2(q-1)} + \sum_{k=1}^{q-1} (t-1)^{q-1-k} t^{2k} \left( \frac{1}{4} \right)^k \right) \left( \sum_{i=0}^{q^2-q} b_i t^i \right). \quad (4.6)
\end{aligned}$$

We let  $\sum_{i=1}^{q^2+q-1} c_i t^i$  denote the right-hand side of (4.6) and write  $d_n := a_n - \frac{n+1}{2^n}$  for integer  $n$  with  $1 \leq n \leq q^2 - 1$ . Then (4.6) tells us that

$$(t^q - t^{q-1} - 1) \sum_{n=1}^{q^2-1} d_n t^n = \sum_{i=1}^{q^2+q-1} c_i t^i. \quad (4.7)$$

By comparing the coefficient of  $t^i$  with  $1 \leq i \leq q^2 + q - 1$  in both sides of (4.7), one obtains the following recursive relations:

$$\begin{cases} c_j = -d_j, & \text{if } 1 \leq j \leq q-1; \\ c_q = -d_1 - d_q; \\ c_{q+j} = d_j - d_{j+1} - d_{q+j}, & \text{if } 1 \leq j \leq q^2 - q - 1; \\ c_{q^2+j} = d_{q^2-q+j} - d_{q^2-q+j+1}, & \text{if } 0 \leq j \leq q-2; \\ c_{q^2+q-1} = d_{q^2-1}. \end{cases}$$

It then follows that

$$\begin{cases} d_j = -c_j, & \text{if } 1 \leq j \leq q-1; \\ d_q = c_1 - c_q; \\ d_{lq+j} = d_{(l-1)q+j} - d_{(l-1)q+j+1} - c_{lq+j}, & \text{if } 1 \leq l \leq q-2 \text{ and } 1 \leq j \leq q-1; \\ d_{lq} = d_{(l-1)q} - d_{(l-1)q+1} - c_{lq}, & \text{if } 2 \leq l \leq q-2; \\ d_{q^2-q+j} = \sum_{i=j}^{q-1} c_{q^2+i}, & \text{if } 0 \leq j \leq q-1. \end{cases} \quad (4.8)$$

One can now give the main result of this section as the conclusion of this paper.

**Theorem 4.1.** *Let  $c_i$  be given as above for  $1 \leq i \leq q^2 + q - 1$ . Then each of the following is true:*

$$\begin{aligned}
& \sum_{a \in \mathbb{F}_q} E_j(1, a) = -c_j + \frac{j+1}{2^j} \text{ if } 1 \leq j \leq q-1; \\
& \sum_{a \in \mathbb{F}_q} E_q(1, a) = c_1 - c_q + \frac{1}{2^q}; \\
& \sum_{a \in \mathbb{F}_q} E_{lq+j}(1, a) = \sum_{a \in \mathbb{F}_q} E_{(l-1)q+j}(1, a) - \sum_{a \in \mathbb{F}_q} E_{(l-1)q+j+1}(1, a) - c_{lq+j} - \frac{2^{q-1}j - j - 1}{2^{lq+j}} \\
& \text{if } 1 \leq l \leq q-2 \text{ and } 1 \leq j \leq q-1; \\
& \sum_{a \in \mathbb{F}_q} E_{lq}(1, a) = \sum_{a \in \mathbb{F}_q} E_{(l-1)q}(1, a) - \sum_{a \in \mathbb{F}_q} E_{(l-1)q+1}(1, a) - c_{lq} + \frac{1}{2^{lq}} \text{ if } 2 \leq l \leq q-2; \\
& \sum_{a \in \mathbb{F}_q} E_{q^2-q+j}(1, a) = \sum_{i=j}^{q-1} c_{q^2+i} + \frac{j+1}{2^{q^2-q+j}} \text{ if } 0 \leq j \leq q-1.
\end{aligned}$$

*Proof.* Since  $\sum_{a \in \mathbb{F}_q} E_n(1, a) = d_n + \frac{n+1}{2^n}$ , then by (4.8), Theorem 4.1 follows immediately.  $\square$

## REFERENCES

- [1] S.D. Cohen, Dickson polynomials of the second kind that are permutations, *Canad. J. Math.* 46 (1994), 225-238.
- [2] X. Hou and T. Ly, Necessary conditions for reversed Dickson polynomials to be permutational, *Finite Fields Appl.* 16 (2010), 436-448.
- [3] X. Hou, G.L. Mullen, J.A. Sellers and J.L. Yucaus, Reversed Dickson polynomials over finite fields, *Finite Fields Appl.* 15 (2009), 748-773.
- [4] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, Second Ed., vol. 20, Cambridge University Press, Cambridge, 1997.
- [5] Q. Wang and J.L. Yucaus, Dickson polynomials over finite fields, *Finite Fields Appl.* 18 (2012), 814-831.